



# Tecnologias de Redes de Comunicações

2006/2007

O protocolo PPP

**Fernando M. Silva**

*Fernando.Silva@ist.utl.pt*

Instituto Superior Técnico

- O protocolo PPP
- Tramas HDLC
- Componentes do protocolo PPP
- Diagrama de estados
- Análise das componentes do protocolo
- Variantes do protocolo PPP

## PPP- Point to Point Protocol

- Ligação directa entre dois nós
- Acesso "dial-up"
- Vantagem: permite a identificação e autenticação do utilizador
- Configuração automática
  - Mecanismo automático que permite a dois terminais negociarem as características
- Meios de acesso
  - Linha série
  - GSM/GPRS
  - ADSL
  - Links rádio
  - Fibra óptica
- Pode encapsular vários protocolos de transporte

## Diagrama de protocolos

---

### Localização do protocolo PPP no modelo OSI



- O protocolo PPP é baseado no protocolo HDLC (High Level Data Link Control)
- Existem muitos outros protocolos baseados em HDLC:
  - SDLC (Synchronous Data Link Control, LLC (Logical Link Control), LAPB (Link Access Control Balanced), LAPD, LPDm, LAPM, LAPF...
- HDLC
  - Norma ISO (International Organization for Standardization) 13239
  - Inicialmente desenhada para suportar ligações multi-ponto ou ponto a ponto
  - Actualmente usada quase exclusivamente para ligações ponto a ponto

## Tramas HDLC

Flag 0x7E 1 byte	Address 1 byte	Control 1 ou 2 bytes	Information data 0 a N bytes	FCS 1 ou 2 bytes	Flag 0x7E 1 byte
---------------------	-------------------	-------------------------	---------------------------------	---------------------	---------------------

- As Tramas HDLC são delimitadas no início e no fim com um byte de flag 0x7E, 0X7E = 01111110
- Address - Permite identificar o destinatário
- Control - Especifica o tipo de frame
- FCS - Fram Control Sequence - Detecção de erro

- Como identificar o campo de flag na stream, caso existam dados com esta configuração?
  - Ligações síncronas (orientada ao bit):  
”bit stuffing” - Inserção de um zero sempre que é detectado uma sequência de 5 uns nos dados
  - Ligações assíncronas (orientadas ao byte):  
”byte stuffing” : Os caracteres especiais são precedidos de um caracter de escape seguido do ”ou exclusivo” do caracter com 20H
    - \* Flag - 7E - 7D 5E
    - \* Escape 7D - 7D 5D
    - \* ETX 03 - 7D 23
    - \* XON 11 - 7D 31
    - \* XOFF 13 - 7D 33
- Questão: qual o formato de uma eventual trama com conteúdo  
”AA 7E 03 7D 7D 45 56 13”?

- Como identificar o campo de flag na stream, caso existam dados com esta configuração?
  - Ligações síncronas (orientada ao bit):  
”bit stuffing” - Inserção de um zero sempre que é detectado uma sequência de 5 uns nos dados
  - Ligações assíncronas (orientadas ao byte):  
”byte stuffing” : Os caracteres especiais são precedidos de um caracter de escape seguido do ”ou exclusivo” do caracter com 20H
    - \* Flag - 7E - 7D 5E
    - \* Escape 7D - 7D 5D
    - \* ETX 03 - 7D 23
    - \* XON 11 - 7D 31
    - \* XOFF 13 - 7D 33
- Questão: qual o formato de uma eventual trama com conteúdo  
”AA 7E 03 7D 7D 45 56 13”?

R. 0F AA 7D 5E 7D 23 7D 5D 7D 5D 45 56 7D 33



# Tramas PPP

---

As tramas PPP utilizam o formato HDLC, herdando deste o formato genérico

Trama HDLC	Flag 0x7E 1 byte	Address 1 byte	Control 1 ou 2 bytes	Information data 0 a N bytes		FCS 1 ou 2 bytes	Flag 0x7E 1 byte
Trama PPP	Flag 0x7E	Address 0xFF	Control 0x03H	Protocol 2 bytes	PPP info 0 a N-2 bytes	FCS 1 ou 2 bytes	Flag 0x7E

O campo protocolo define o tipo de trama do protocolo PPP.

## Componentes do protocolo PPP

---

O protocolo PPP tem quatro tipos de tramas, algumas delas correspondendo a sub-protocolos utilizados para estabelecer uma ligação PPP:

- O protocolo LCP (Link Control Protocol) permite iniciar a ligação, testar a linha, negociar opções de configuração e terminar a ligação.
- O protocolo NCP (Newtork Control Protocol), que permite multiplexar diversos protocolos da camada de rede (p. ex., IP, IPX, Apple Talk...)
- Protocolos de autenticação (por exemplo, CHAP e PAP)

<b>LCP</b>	<b>NCP</b>	<b>PAP/CHAP</b>	<b>Data</b>
<b>HDLC</b>			

## Valores do campo de protocolo PPP

---

Lista não exaustiva de valores possíveis do campo protocolo

- 0xC021 LCP - Link Control Protocol
- 0xC023 PAP - Password Authentication Protocol
- 0xC025 LQR - Link Quality Report
- 0xC223 CHAP - Challenge Handshake Protocol
- 0x8021 IPCP - IP control protocol
- 0x80FD CCP - Compression Control Protocol

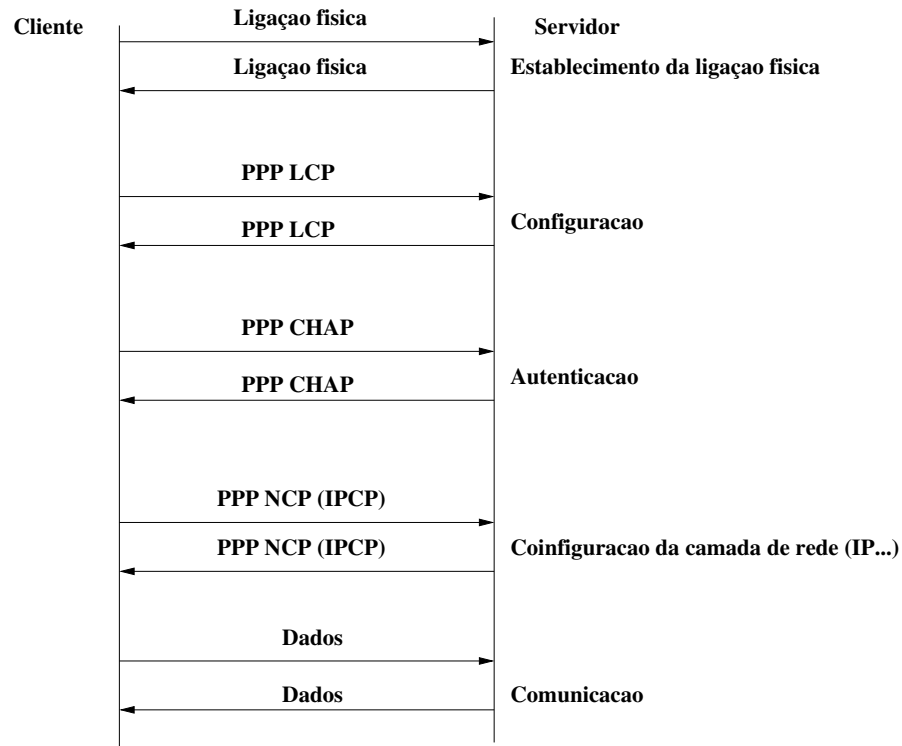
A Microsoft usa uma subopção do CCP para permitir tramas cifradas de PPP usando o algoritmo MPPE. O protocolo PPP-MPPE é usado pela Microsoft é usado para o estabelecimento de VPNs e é hoje também suportado em Linux (e usado, p. ex. na rede sem fios na Alameda).

- 0x0800 Dados IP

# Estabelecimento de uma ligacao IP em PPP

---

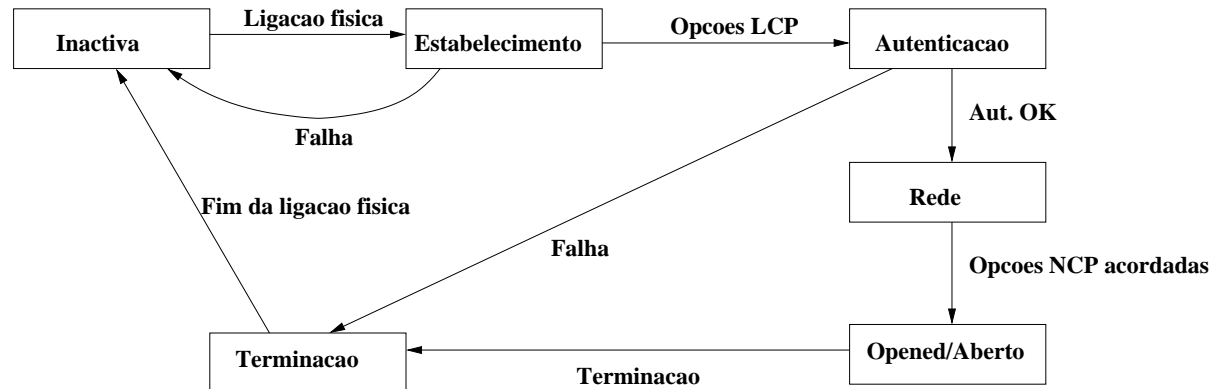
## Fases do protocolo PPP



## Diagrama de estados

---

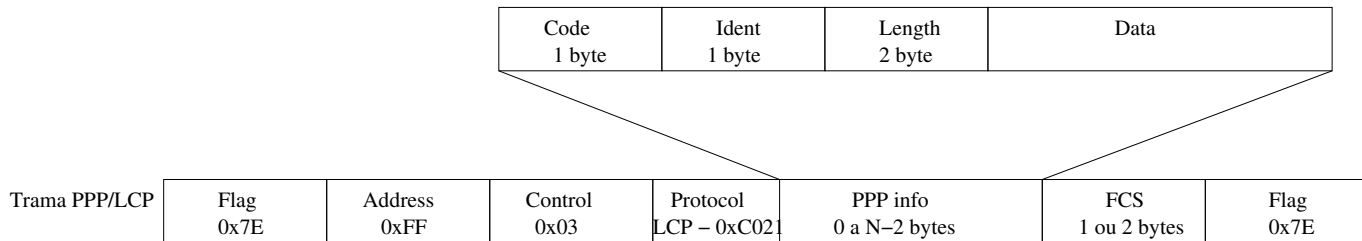
### Diagrama de estados do protocolo PPP



# Link Control Protocol

---

## Formato da Trama LCP



- Code - Define o código de operação
- Ident - Sequência das mensagens (numeração que permite associar pedidos e respostas)
- Length - Auto explicativo

- Valores possíveis: Configure-Request, Configure-Ack, Configure-Nak, Configure-Reject, Terminate-Request, Terminate-Ack, Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply, identification, Time-Remaining
- Os pacotes Configure-Request e Configure-Ack têm como função negociar as opções de configuração, enquanto que a maioria dos restantes códigos servem sobretudo para controlar o estado da ligação.
  - Configure-Request - Envio das opções (do terminal para o receptor)
  - Configure-Ack - OK (do receptor para o terminal)
  - Configure-Nak - Valor da opção não suportado pelo receptor
  - Configure-Reject - Opção não suportada

- O campo de dados das tramas "configure" do LCP tem por sua vez um tipo, comprimento, e informação.
- O tipo permite especificar as opções suportadas:  
Maximum Receive Unit, Authentication Protocol, Quality Protocol Report, Magic Number, Protocol Field Compressor, Address and Control Field Compression, FCS.
- O transmissor e receptor devem acordar num conjunto de opções suportados por ambos os terminais.



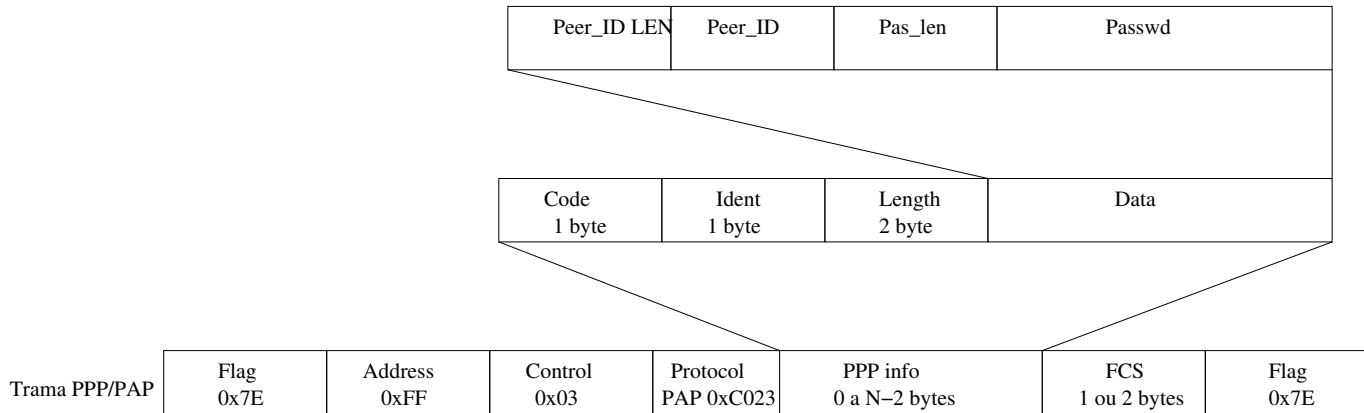
O PPP suporta dois tipos básicos de autenticação:

- PAP - Password Authentication Protocol
  - Neste protocolo o cliente envia simplesmente uma trama com um username e uma password e aguarda-se uma resposta com a confirmação ou rejeição das credenciais
- CHAP - Challenge Handshake Authentication Protocol
  - Neste protocolo, o servidor envia um "challenge", e o equipamento cliente envia uma resposta calculada em função da senha (password) e de um algoritmo de cifra de via única (one hash key). O servidor verifica se o resultado do cálculo remoto e local coincidem e, neste caso, a autorização é confirmada.

# PAP - Password authentication protocol

---

## Trama de PAP

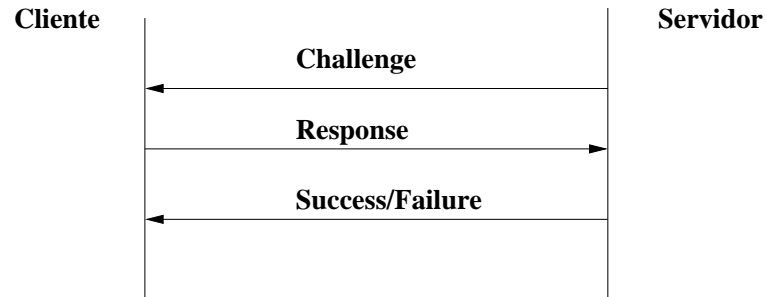


Valores possíveis do campo Code:

- 1 - Authenticate-request
- 2 - Authenticate-ack
- 3 - Authenticate-nak

# CHAP - Challenge Handshake Authentication Protocol

---



Valores possíveis do campo Code:

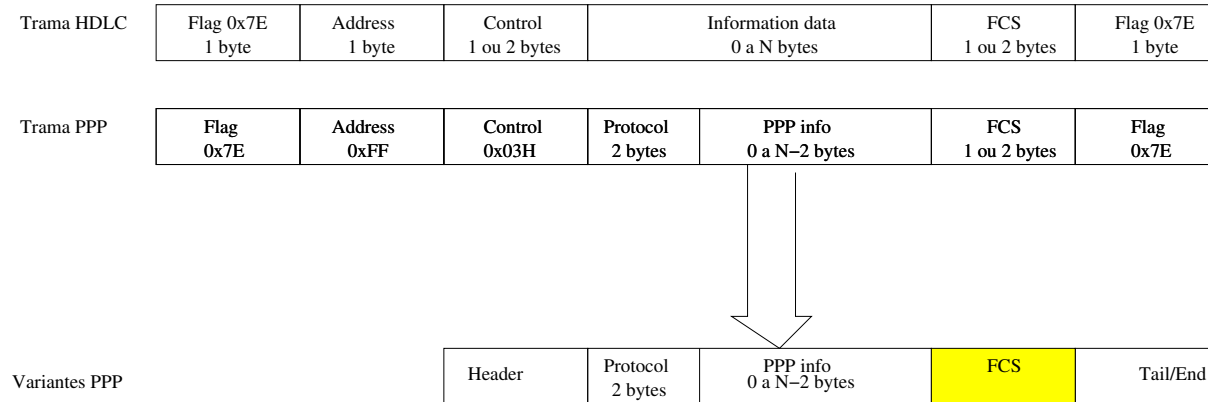
- 1 - Challenge
- 2 - Response
- 3 - Success
- 4 - Failure

- Como referido anteriormente, o protocolo NCP permite negociar os parâmetros de rede a usar durante a fase de transporte.
- O protocolo NCP é agnóstico quanto ao protocolo de rede. No entanto, o protocolo é hoje quase exclusivamente usado para o estabelecimento de ligações IP, pelo que a negociação é neste caso realizada pelo IPCP (IP Control Protocol).
- Código de protocolo 0x8021
- Valores possíveis do campo code:
  - Configure-req, configure-ack, configure-nak, configure-rej, terminate-req, terminate-ack, code-rej
  - Principais Opções de configuração: IP Compression Protocol, IP Address, Primary DNS, Secondary DNS
    - \* A compressão de protocolo, particularmente importante em links de baixo débito, permitia reduzir a dimensão do cabeçalho dos pacotes IP de 40 para 3 bytes.

- O protocolo PPP generalizou-se enquanto forma simples de, simultaneamente,
  - Permitir realizar ligações ponto a ponto
  - Permitir a negociação de opções de ligação e de detalhes de rede
  - Permitir a autenticação (e billing, se for caso disso) do cliente/equipamento remoto
- O protocolo PPP foi inicialmente concebido a pensar sobretudo nas linhas série "lentas", com comunicação através de modem.
- A evolução destas ligações para banda larga implicou que o modelo inicial PPP, em que o protocolo assenta directamente no nível físico, deixou de ser válido.
- No entanto, atendendo às vantagens demonstradas pelo protocolo PPP e ao muito software já desenvolvido com base neste protocolo, surgiram posteriormente várias variantes adaptados a diferentes tipos de nível físico e de ligação.
- Todas estas variantes se baseiam no encapsulamento das componentes "protocol" e "information".

# Variantes do protocolo PPP

---



Nos protocolos derivados do PPP o formato da trama depende do protocolo de dados ou de rede usado.

## Variantes do protocolo PPP

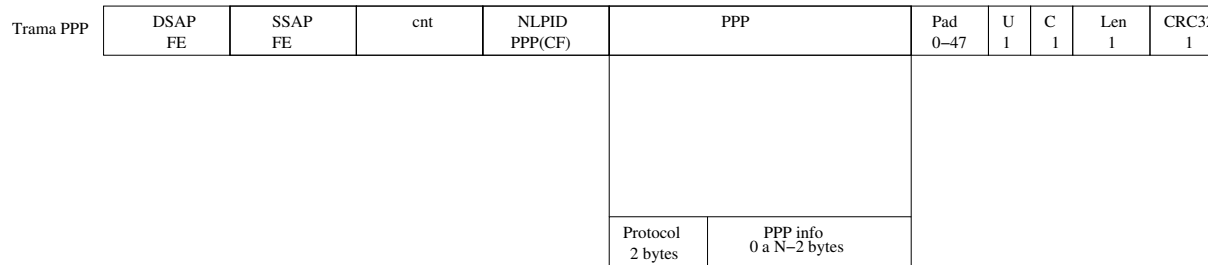
---

- RFC 1618 - PPP sobre RDIS
- RFC 1598 - PPP sobre X25
- RFC 2364, RFC 3336 - PPP sobre ATM
- RFC 2516 - PPP sobre Ethernet (PPPoE)

# PPP sobre AAL5

---

## Exemplo: PPP sobre ATM/AAL5



DSAP - Destination Service Access Point

SSAP - Source Service Access Point



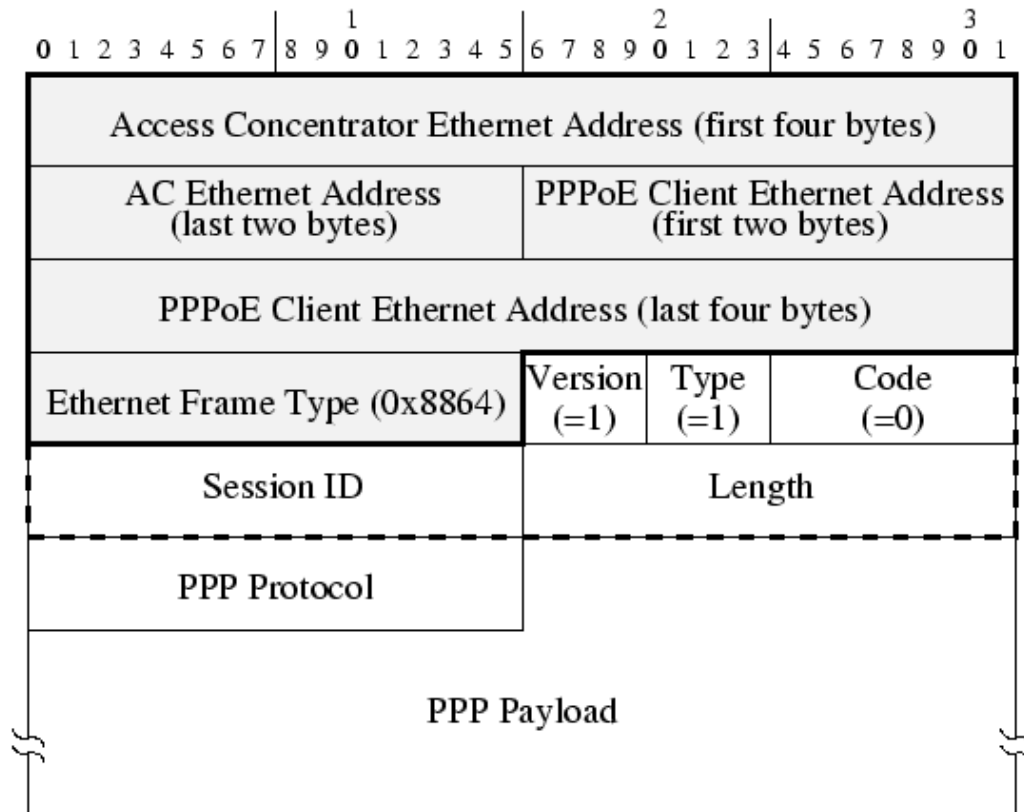
## PPP sobre Ethernet

- Com a introdução das redes de banda larga, o acesso passou frequentemente a ser realizado através de ligações multi-ponto, com um acesso partilhado.
- O PPP foi desenvolvido inicialmente para ligações ponto a ponto
- O protocolo PPPoE (PPP over Ethernet) permitiu estender este protocolo a ligações multi-ponto sobre ethernet.
- Normalmente, vários terminais são ligados a um mesmo concentrador remoto

- Problemas da extensão do protocolo a uma ligação multi-ponto:
  - Como encontrar o par remoto (concentrador)?
- PPPoE inclui esta facilidade e a permite estabelecer um identificador de sessão único.
- O PPPoE divide-se em duas fases distintas:
  - Fase de descoberta
    - \* Fase em que se encontra o par de comunicação e estabelecimento do identificador de sessão
  - Fase de sessão
    - \* Fase em que o terminal e o concentrador utilizam uma interface virtual PPP para realizar uma ligação ponto a ponto.

## PPP sobre Ethernet

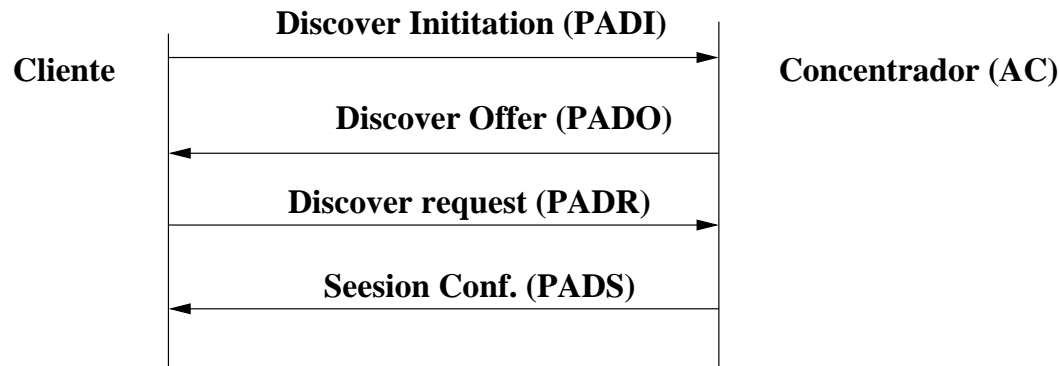
Formato da trama Ethernet nmo protocolo PPPoE



## Fase de descoberta

---

- O terminal transmite em broadcast um pacote de iniciação (PPPoE Active Discover Initiation, PADI)
- Um (ou mais) concentradores de acesso (AC) emitem pacotes de oferta (PPPoE Active Discover Offer, PADO)
- O terminal emite um pacote de pedido de sessão em unicast ao concentrador de acesso selecionado (PPPoE Actived Discover Request, PADR)
- O concentrador emite um pacote de confirmação (PPPoE Active Discover Session Confirmation, PADS).



- IPoE: IP over Ethernet
- Acesso por DHCP+IP convencional
  - Limitações: ausência de autenticação, acesso ao meio antes de autenticação
  - É possível realizar autenticação em níveis superiores (ver acesso wireless com autenticação web no IST), mas o acesso não autenticado ao meio pode permitir já problemas ou perturbações com origem difícil de localizar.
  - Solução: 802.1X com autenticação EAP e cifra de dados (acesso semelhante ao que hoje em dia existe na rede sem fios e-U/eduroam).
  - O 802.1X é hoje suportado pela maioria do equipamento de distribuição (switchs) de uso profissional (designados switchs com gestão ou "managed switchs").
- Problema: o equipamento de acesso (sobretudo doméstico) nem sempre suporta 802.1X